IERP Data Handling Manual
April 2015

Recent legislation requires educational institutions to develop and implement longitudinal data systems that support data-driven decision making and increase research on student achievement.

In compliance with these initiatives, Cerritos College has developed a data warehousing system and guidelines to accompany its use. Those guidelines are discussed in this handbook and cover topics such as proper use, storage, and maintenance of student data records.
# Table of Contents

Access to Data ................................................................................................................................. 1
  Who Has Access? .......................................................................................................................... 1
  How Can Departments Request Data? .......................................................................................... 2
  IERP Data Use ............................................................................................................................ 2

Data Security ................................................................................................................................... 3
  Sensitive Information .................................................................................................................... 3
  Keeping Sensitive Information Safe ............................................................................................ 4

Data Storage and Archiving .......................................................................................................... 5
  Active and Inactive Data ............................................................................................................... 5
  Data Destruction .......................................................................................................................... 5
  Unauthorized Storage ................................................................................................................... 5

Transferring Data ............................................................................................................................ 8
  IERP Data Transfer Process ........................................................................................................ 8

Data Breach ..................................................................................................................................... 9
  What To Do If Data Is Compromised .......................................................................................... 9
  Outcomes Of A Data Breach ........................................................................................................ 9

Data Validation and Integrity ......................................................................................................... 10
  Guaranteeing High Quality Data ................................................................................................. 10
  Dealing With Data Errors .......................................................................................................... 11
  Building Quality Assurance Into Work ...................................................................................... 11

References ...................................................................................................................................... 12

Additional Resources ..................................................................................................................... 13
Access to Data

Who Has Access?

The U.S. Department of Education requires all staff and contractors with access to Personally Identifiable Information (PII) to undergo a security screening. The screening might include a background investigation using written, electronic, telephone, or personal contact to determine the suitability, eligibility, and qualifications of a staff member for employment. (Guidance for Statewide Longitudinal Data Systems, 2010, p.9)

Only Cerritos College staff members who have been properly screened are allowed access to secured data.

The Institutional Effectiveness, Research, and Planning Office

The IERP Dean has full access to institutional data and administers access-levels to his/her team of employees. To ensure data security, the IERP Dean will also:

- Coordinate the data collection process
- Resolve discrepancies in information before reports are disseminated
- Establish data auditing responsibilities
- Develop a calendar for data collection and reporting
- Develop and disseminate data entry standards
- Develop a process that allows staff to request new reports or modifications of existing reports
- Collaborate with curriculum coordinators and staff from other educational program areas on data related matters
- Collaborate with the Director of IT to address data integrity and appropriate reporting tools
- Provide professional development for staff members leading toward a culture of quality data

Adapted from National Forum on Education Statistics, 2004, P.31

IERP Research Analysts and Assistants

The IERP Dean will keep a record of the authorization levels he/she administers to each IERP employee. All IERP employees will also sign an Affidavit of Nondisclosure (see Attachment D) in which they are made aware of:

- PII laws, rules, and procedural protections
- A pledge to protect the personally identifiable data in each student’s education record
- Penalties for violations
How Can Departments Request Data?

1. College employees can submit a request for research or data -via the IERP website’s “request” service: [http://cms.cerritos.edu/research-and-planning/webpage-update-4.30.2015/research-request.htm](http://cms.cerritos.edu/research-and-planning/webpage-update-4.30.2015/research-request.htm)

2. When the request is received, it is reviewed and approved by the IERP Dean.

3. Upon approval, the IERP Dean will assign the data request to an IERP staff member for completion.

4. Non-employees can request data using the Public Record Request form (see appendix E).

   Note: Public Record Requests require the president’s approval for completion and will be filled using existing data.

IERP Data Use

Program Evaluation and Audits
IERP staff use PII from educational records to audit or evaluate a federal-or state supported “educational program,” or to enforce, or comply with, federal legal requirements related to an educational program. As specified by FERPA regulations, §99.3, “an education program must be principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution.”

Other Uses

In addition to program evaluations, IERP staff may use student education records for:

1. **OPERATIONS REPORTS**
   Data is reviewed to ensure the efficiency of day-to-day school functions like attendance, records management, special needs education offerings, and the delivery of health services or transportation programs.

2. **MANAGEMENT REPORTS**
   Data is used for planning and scheduling educational programs or for the distribution of financial resources.

3. **ACCOUNTABILITY REPORTS**
   Data is used to provide school boards and other education agencies with information about student accomplishments, the effectiveness of staffing levels, or the progress of specific educational programs.

4. **RESEARCH & EVALUATION REPORTS**
   Data is used to conduct an analysis of the success of student subgroups, changes in achievement over time, or to identify effective instructional strategies and promote school improvement.

Adapted from National Forum on Educations Statistics, 2004, p. 44
Sensitive Information

The IERP office uses student personal information for purposes discussed in the “IERP Data Use” section of this manual. As a result, student records in IERP may contain direct identifiers such as: name, address, social security number, other unique education-based identifiers, photographs, or fingerprints.

Records may also contain indirect identifiers -not unique to a student or his/her family but can be used in combination with other information to identify them (e.g., racial or ethnic identity, date of birth, place of birth, mother’s maiden name, grade level, participation in a specific program, course enrollment).

An unauthorized release of direct or indirect student identifiers could lead to the harm or embarrassment of a student. To prevent such a data breach from occurring, it is important to follow a strict security policy that protects students’ right to privacy.
# Keeping Sensitive Information Safe

In compliance with regulations that govern student Personally Identifiable Information (PII), IERP staff will take the following precautions when handling student data:

## Data
- **Aggregation:** coarsen categorical data, e.g., don’t release geographic units under 100,000 people
- **Top-coding:** report values (e.g., incomes, ages) above thresholds only as "above the threshold"
- **Data Swapping:** switch one record’s values on key variables with another record’s values
- **Micro-aggregation:** cluster numerical data (e.g., incomes) in groups of at least three records
- **Multiple imputation for disclosure limitation** (also called synthetic data): replace sensitive values with simulated values drawn from statistical models

Adapted from American Statistical Association Committee on Privacy and Confidentiality, 2011

## Password Protection
- Keep passwords strictly confidential
- Change passwords every 30 to 60 days
- Create passwords containing both numbers and letters using upper/lower casing
- Learn the passwords or store them somewhere private and secure
- Don’t use passwords identifying a personal fact about yourself (i.e. DOB, child’s name)

Adapted from National Forum on Education Statistics, 2007, p.46

## Physical Security
- Send PII by email only –after using an encryption program
- Put confidential information into a locked cabinet or drawer when leaving the area where it is used
- Lock desks, offices, and filing cabinets where PII is stored
- Hold all conversations regarding confidential PII in private/secure areas
- When recycling computers, clean or reformat hard drives
- Don’t work on confidential data from a home/personal computer
- Position desks to maximize privacy of materials on work surfaces
- Make sure computer screens do not face public areas

## Technical Practices
- Make sure wireless networks are secure
- Implement an appropriate backup system
- Establish a plan for reacting to data security breaches
- When deleting confidential materials, use overwriting software to ensure data is completely deleted
- Periodically audit security processes
Data Storage and Archiving

Active and Inactive Data

Primary Storage
During program reviews, institutional reports, grant reports, etc. IERP active data will be stored on a password protected shared network drive – accessible only to the IERP Dean, analysts and research assistants with appropriate access credentials. Campus IT assigns a drive letter to each authorized machine that needs to access the shared drive. Campus IT is responsible for the periodic backup of data on the shared drive.

Secondary Storage
The archive schedule of data on the IERP network drive is governed by deadlines associated with institutional or grant reporting processes.

Following the completion of a grant report, institutional report, or program review, active-working data must be migrated from the IERP network drive to a secure external hard drive. It is kept on the external hard drive for up to six years. The external hard drive ensures that inactive data is kept separate from the currently active components of an electronic record, to decreases the likelihood of unauthorized or inadvertent disclosure and to afford storage space on the shared network drive.

The external password encrypted hard drive is kept under lock and key in the IERP Office. Files contained in the hard drive receive periodic and cyclical updates and/or deletions.

Data Destruction

Once it has been determined by the IERP Dean that a file is no longer necessary for program reporting, institution reporting, grant reporting, audits, for enforcement, or compliance activity, the file is to be destroyed in a manner that protects the privacy and confidentiality of the individuals involved.

The process for destruction of IERP Sensitive data is as follows:

1) All printed materials must be visually inspected for PII prior to shredding. Anywhere PII is found it must be overridden in black sharpie ink. After eliminating all sensitive information on a document, it can be shredded.
2) All digital materials approved for destruction must be permanently deleted across all storage platforms. This can be done using the digital shredding software.
3) In cases where board approval is required for data destruction, the IERP Dean should be contacted prior to destruction. These files typically include college published data.

Unauthorized Storage

IERP data cannot be saved as a local copy on a personal or work computer unless authorized by the IERP Dean. Data must remain on the Research shared network drive when active, or archived in a password encrypted hard drive when inactive. This measure decreases the likelihood of unauthorized or inadvertent disclosure of PII.
IERP records can typically be classified into one of four categories: highly restricted, confidential, internal, or public. Depending on the classification level of a record, IERP staff can also decide where to store it, aside from the network drive.
**Data Classification and Storage Chart**

<table>
<thead>
<tr>
<th></th>
<th>Level 0 - Public</th>
<th>Level 1 - Internal</th>
<th>Level 2 - Confidential</th>
<th>Level 3 – Highly Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerritos Owned Workstations, Laptops, Tablets, other devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Publicly Accessible Kiosks and Workstations</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personally Owned Workstations, Laptops, Tablets, other devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ITS-Provided Network Drives (Z:, W:, S:, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cerritos Email</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Cloud Storage Sites (e.g., Dropbox)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cerritos websites (including departmental websites, etc.)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cerritos Survey Share Service</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portable Electronic Storage Media, such as USB devices, CD/DVD, or external hard drives.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Data classification levels:
- **Level 0 - Public**: Data is made available to the public.
- **Level 1 - Internal**: Data is intended for a designated workgroup, or department and is not protected by statute or regulation.
- **Level 2 - Confidential**: Data is intended for a very specific use and should not be disclosed except to those who have explicit authorization to review such data.
- **Level 3 – Highly Restricted**: Data is protected by specific statutes, standards, or agreements with specific provisions dictating how this type of data must be protected.
Transferring Data

The IERP Data Transfer Process

IERP staff are required to keep a brief account of how each of their reports will use PII (i.e., to complete an audit, evaluation, enforcement, or compliance activity). IERP staff records should specify that the purpose for which they are releasing PII to an authorized representative is to carry out an audit or evaluation of federal-or state-supported education programs, or to enforce or comply with federal legal requirements that relate to those programs.

IERP staff also acknowledge that in disclosing PII to an entity, they are in no way assigning ownership of the PII to that entity. Re-disclosure of PII may only happen with the permission of the IERP Dean or otherwise in compliance with FERPA and its regulations.

Data Release Rules
The table below contains examples of reports released by the IERP office, on a quarterly or yearly basis, to outside campus departments and/or state and federal organizations. The following rules will be observed by IERP staff during the reporting or data transfer process.

### Data Transfer Examples

<table>
<thead>
<tr>
<th>Report</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Review Information</td>
<td>Campus Departments</td>
</tr>
<tr>
<td>Award Count</td>
<td>Campus Departments</td>
</tr>
<tr>
<td>Gainful Employment</td>
<td>Federal</td>
</tr>
<tr>
<td>Service Area High School</td>
<td>State/President’s Office</td>
</tr>
<tr>
<td>Yield Counts</td>
<td></td>
</tr>
<tr>
<td>IPEDS Fall/Winter/Spring</td>
<td>Federal</td>
</tr>
<tr>
<td>Collection</td>
<td></td>
</tr>
<tr>
<td>ACT-On (grant reporting)</td>
<td>Federal/DOL</td>
</tr>
<tr>
<td>STEM (grant reporting)</td>
<td>Federal</td>
</tr>
<tr>
<td>ACCJC Annual Report</td>
<td>ACCJC</td>
</tr>
<tr>
<td>HSI Certification Data</td>
<td>Federal</td>
</tr>
<tr>
<td>Scorecard Board presentation</td>
<td>State</td>
</tr>
<tr>
<td>Veteran students</td>
<td>Federal</td>
</tr>
<tr>
<td>SB70</td>
<td>State</td>
</tr>
<tr>
<td>I.E.P.I</td>
<td>State</td>
</tr>
<tr>
<td>CTE Launch board</td>
<td>State</td>
</tr>
<tr>
<td>Equity</td>
<td>State</td>
</tr>
<tr>
<td>SSSP</td>
<td>State</td>
</tr>
<tr>
<td>Pre-Req Validation</td>
<td>State</td>
</tr>
<tr>
<td>Math Placement Valid</td>
<td>State</td>
</tr>
<tr>
<td>Engl Placement Valid</td>
<td>State</td>
</tr>
<tr>
<td>ESL Placement Valid</td>
<td>State</td>
</tr>
<tr>
<td>Title IX</td>
<td>State</td>
</tr>
</tbody>
</table>

Transfer Rules

- Hardcopy transfer of data will not include any student IDs or other identifying information, and will be transferred on a secured, password-protected drive.
- When transferring data that includes PII by email, turn password protection on in the source document.
- Aggregated data without PII can be emailed without password protection.
- Data disseminated to outside sources, for purposes other than federal/state reporting, may not contain any IDs or other identifying information.
- Program review files can be public.
- Data will be delivered in its required or appropriate file format. Large data will be compressed using WinZip. Instructions on how to retrieve the data will be sent via email to the requestor.
**What to Do If Data Is Compromised**

When a breach occurs, the IERP Dean will conduct an assessment of the potential harm to affected individuals. This assessment will inform whether notification [to affected individuals] is required. The IERP Dean will also include in the assessment a description of the circumstances that resulted in the breach so that procedures may be modified as quickly as possible to avoid future breach.

IERP staff will also be required to fill out a Breach Report Form (attachment C). The form is based on recommendations from the National Institute of Standards and Technology 2010 Guide (p. 5-2—5-4).

**Outcomes of a Data Breach**

IERP staff are required to safeguard data (especially containing student PII) against loss, unauthorized access or use, destruction, modification, or unintended and inappropriate disclosures. To ensure this, they must follow the rules and regulations provided to them during security training and also explained in this manual.

Should a known or suspected breach occur, IERP staff will report it as quickly as possible to appropriate officials in an effort to alleviate adverse effects resulting from the breach. For students, adverse effects may include: identity theft, discrimination, or emotional distress. The related harm to Cerritos College could include loss of public confidence and public reputation, administrative burden of investigating the breach and ensuring necessary remedial steps are taken, and financial losses.
Guaranteeing Data Quality

Data quality is crucial to the success of the IERP office on the Cerritos College campus. IERP support the college’s decision-making, strategic planning, and assessment. To ensure the continuous reliability of IERP reports, IERP staff will closely monitor the way data is entered, stored, and managed through data quality assurance practices. These practices generally include updating, standardizing, and restructuring records stored in multiple disparate systems. IERP staff are also required to introduce the following measures into their work-load, thus ensuring the quality of their data.

### Personal Measures

- Set aside certain times to focus on critical data entry
- Maintain access to and understanding of documentation regarding data entry and data correction procedures, including protocols for handling exceptions (e.g., student won’t provide complete information)
- Check data against authoritative source of data
- Provide data entry reference sheet based on data dictionary
- Provide detailed documentation specific to software
- Run periodic data verification reports
- Provide ongoing training (best practices, data-elements updates, timelines, procedure changes) to all appropriate staff

### Environmental Measures

- Position work space to minimize visual, traffic, and other distractions
- Maintain appropriate and up-to-date software and hardware
- Include basic edit checks in software
- Train data entry staff
- Use “Team” approach/effort for collecting/reporting
- Provide a supportive and safe environment for asking questions and resolving issues

Adapted from National Forum on Education Statistics, 2007, p.62
Dealing With Data Errors

When IERP staff encounter inaccurate, incomplete, or inconsistent data they must immediately begin a correction procedure or check with colleagues on possible solutions. Depending upon the criticality of the error, IERP staff will also be required to submit a report to the IERP Dean, or IT Director, with the following information:

<table>
<thead>
<tr>
<th>Date</th>
<th>Date to Deliver Error Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Decision</td>
<td>Time Needed to Create Error Report</td>
</tr>
<tr>
<td>Staff to Correct Errors</td>
<td>Date for Data Auditing</td>
</tr>
<tr>
<td>Time Needed to Correct Errors</td>
<td>Elements of Data Audit</td>
</tr>
</tbody>
</table>

Building Quality Assurance into Work

The diagram below illustrates how quality data is achieved through periodic audits. Audits help to substantiate individual data elements or identify inaccuracies for correction. Through continuous screening, errors can be caught early and avoid burrowing themselves into different levels of the data collection, reporting, and release process.

*National Forum on Education Statistics, 2007, p.85*
References


### Attachment A.

Under the FERPA regulations at 34 CFR § 99.31, a school may disclose PII from education records without consent when:

- The disclosure is to school officials who have been determined to have legitimate educational interests;
- The disclosure is to other school officials, including teachers, within the agency or institution who have legitimate educational interests; a third-party contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services for which the agency or institution would otherwise use employees—as long as that third party’s use and maintenance of education records is under the direct control of the agency or institution and is subject to the regulation requirements governing the use and redisclosure of PII from education records (34 CFR § 99.33(a));
- An educational agency or institution uses reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests (34 CFR § 99.31(a)(1));
- The disclosure is to officials of another school, district, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student’s enrollment or transfer (34 CFR §§ 99.31(a)(2) and 99.34);
- The disclosure is to authorized representatives of the Comptroller General of the United States, the Attorney General of the United States, the Secretary of the Department of Education, or state and local educational authorities for the purpose of auditing or evaluating federal or state supported education programs or enforcing federal laws which relate to those programs (34 CFR §§ 99.31(a)(3) and 99.35);
- The disclosure is in connection with financial aid for which the student has applied or which the student has received if the information is necessary for such purposes as to determine eligibility, the amount, the conditions for the student to apply for or receive financial aid or enforce the terms and conditions of the aid (34 CFR § 99.31(a)(4));
- The disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions for specified purposes related to predictive tests, student aid programs, or the improvement of instruction (34 CFR § 99.31(a)(6));
- The disclosure is to accrediting organizations to evaluate accreditation status (34 CFR § 99.31(a)(7));
- The disclosure is pursuant to a court order or a lawfully issued subpoena 18 (34 CFR § 99.31(a)(9));
- The disclosure is in connection with a health or safety emergency (34 CFR §§ 99.31(a)(10) and 99.36);
- The information disclosed has been appropriately designated as directory information by the school (34 CFR § 99.31(a)(11) and 99.37);
- The disclosure is of de-identified student level data for the purposes of education research (34 CFR § 99.31(b)).

Adapted from [Guidance for Statewide Longitudinal Data Systems, 2010, p.15](#).
Attachment B.

**MULTIPLE MEASURES OF DATA**

Allows the prediction of actions/processes/programs that best meet the learning needs of all students.

Over time, demographic data indicate changes in the context of the school.

Tells us: What processes/programs different groups of students like best.

Tells us: If groups of students are "experiencing school" differently.

Tells us: The impact of demographic factors and attitudes about the learning environment on student learning.

**DEMOGRAPHICS**

- Enrollment, Attendance, Drop-Out Rate
- Ethnicity, Gender, Grade Level

**SCHOOL PROCESSES**

- Description of School Programs and Processes

Tells us: What processes/programs work best for different groups of students with respect to student learning.

Tells us: If a program is making a difference in student learning results.

**PERCEPTIONS**

- Standardized Tests
- Norm/Criterion-Referenced Tests
- Teacher Observations of Abilities
- Authentic Assessments

Perceptions of Learning Environment Values and Beliefs

Over time, perceptions can tell us about environmental improvements.

Tells us: The impact of student perceptions of the learning environment on student learning.

Tells us: The impact of the program on student learning based upon perceptions of the program and on the processes used.

**STUDENT LEARNING**

Over time, student learning data give information about student performance on different measures.

## Data Breach Report Form

<table>
<thead>
<tr>
<th><strong>FIELD NAME</strong></th>
<th><strong>COMMENTS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME, JOB TITLE, AND CONTACT INFO OF THE PERSON WHO DISCOVERED THE INCIDENT</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>NAME, JOB TITLE, AND CONTACT INFO OF THE PERSON REPORTING THE INCIDENT</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>DATE AND TIME THE INCIDENT WAS DISCOVERED</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>NATURE OF THE INCIDENT (e.g., system level electronic breach, an electronic breach of one computer or device, or a breach of paper extracts of records)</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>BRIEF DESCRIPTION OF THE INFORMATION LOST OR COMPROMISED</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>NAME OF ELECTRONIC SYSTEM BREACHED AND POSSIBLE INTERCONNECTIVITY WITH OTHER SYSTEMS</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>STORAGE MEDIUM FROM WHICH INFORMATION WAS LOST OR COMPROMISED</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>CONTROLS IN PLACE TO PREVENT UNAUTHORIZED USE OF THE LOST OR COMPROMISED INFORMATION</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>NUMBER OF INDIVIDUALS POTENTIALLY AFFECTED</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>WAS LAW ENFORCEMENT CONTACTED</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>IS BREACH NOTIFICATION TO AFFECTED INDIVIDUALS REQUIRED</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>WHO SHOULD RECEIVE NOTIFICATION OF THE BREACH (e.g., law enforcement, financial institutions, affected individuals, media, the general public).</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>TIMELINESS OF THE NOTIFICATION</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>GENERAL CONTENT OF THE NOTIFICATION</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>SOURCE OF THE NOTIFICATION (e.g., principal, Superintendent, school board)</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>MEANS OF PROVIDING THE NOTIFICATION (e.g., letter or public announcement)</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>REMEDIATION OPTIONS TO BE PROVIDED -if any (e.g., a free copy of credit report, credit monitoring)</td>
<td>Click here to enter text.</td>
</tr>
</tbody>
</table>

Revised 2/25/2015 by E. Arias
Attachment D.
Affidavit of Nondisclosure
For the use of Sensitive Data

I, ___________________________, through my involvement with the Institutional Effectiveness, Research, and Planning office at Cerritos College will have access to personnel and student personally identifiable information (PII). By virtue of my affiliation with the IERP office, I have access to confidential information generally perceived as personal and private. I understand that access to this confidential information and data carries with it responsibility to guard against unauthorized use. To treat information confidentially means to not divulge it, or cause it to be accessible to anyone who is not properly screened or approved to use it. Anything not specifically named as “public information” is considered confidential.

I understand that inappropriately disclosing, or allowing unauthorized access to data from the Institutional Effectiveness, Research, and Planning office is subject to criminal prosecution and/or civil recovery and violates the Cerritos College code of ethics.

Federal and state laws that govern student and personnel PII include, but are not limited to:
- The Family Educational Rights and Privacy Act
- Protection of Pupil Rights Amendment
- California Constitution, Article 1 (Sect.13)
- Gramm-Leach-Bliley Act
- Individuals with Disabilities Education Act

These regulations dictate the obligations that institutions have with regards to data “privacy,” “personally identifiable information,” “disclosure,” “access,” and “confidentiality.”

I agree to fulfill my confidentiality responsibilities in accordance with the following guidelines:

1. I agree not to permit unauthorized access to these sensitive data, in either electronic or paper copy.
2. I agree not to attempt to identify individuals, families, households, schools, or institutions.
3. I agree that if the identity of an individual, family, household, school or institution is discovered inadvertently, I will a) make no use of this knowledge, b) advise the IERP Dean of the incident c) safeguard or destroy the information as directed by the IERP Dean, and d) not inform any other person of the discovered identity.

______________________________    ______________________________
Name                            Date

______________________________    ______________________________
Signature                        Cerritos Email
## Attachment E.
Public Records Request Form

<table>
<thead>
<tr>
<th>Date of Request</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestor Name</td>
<td></td>
</tr>
<tr>
<td>Co./ Department</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
</tbody>
</table>

**REASON(S) FOR REQUEST**

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

**IERP ACTION ON PUBLIC RECORD REQUEST**

- [ ] Granted in full (records(s) enclosed)
- [ ] Denied in full; reason for denial
- [ ] Granted in part; denied in part/reason

---

Submit form to: Dr. Kristi Blackburn, IERP Dean, 562.860.2451 x2193, LC-121
E-mail: kblackburn@cerritos.edu

IERP Dean, Cerritos College